Research Note: RSA 2020

Rajeev Chand
Partner and Head, Research
rajeev@wing.vc

Olivia Rodberg
Research Associate
olivia@wing.vc

Wing Venture Capital
480 Lytton Avenue
Palo Alto, CA 94301

The 29th annual RSA Conference was held February 24-28, 2020, at the Moscone Center in San Francisco. The conference is one of the largest security industry gatherings globally with approximately 40,000 attendees. Due to COVID-19 concerns, this year's conference was less well attended than last year's; however, the conference was still busy and productive.

At this year's conference, Wing moderated a keynote, held the second annual Wing Summit: Security, co-hosted the Evening Reception, and held private meetings with security leaders:

- We moderated the Keynote on "Genomics: A New Frontier for Security and Privacy" with Patrick Courneya, Chief Medical Officer at Kaiser Permanante, Kathy Hibbs, Chief Legal and Regulatory Officer at 23andMe, Mike Wilson, Chief Security Officer at Molina Healthcare, and Sharon Terry, CEO of Genetic Alliance.
- We held the second annual Wing Summit: Security, an exclusive, invitation-only dialogue with 100 chief security officers and chief information security officers at Fortune 500 corporations and modern tech companies. This year's summit featured a government fireside chat and a board of director roundtable with three board members from public companies with recent, high-profile breaches.
- Wing co-hosted the Evening Reception at the Jewish Contemporary Museum with over 350 cybersecurity executives, entrepreneurs, and venture capitalists.
- Wing's research team held 40 1:1 private meetings with security practitioners over four days, principally including chief- and vice president-level executives to discuss observations from RSA and trends and unsolved problems in cybersecurity.

Our takeaways included:

1) Boards and Security. As discussed in last year's research note, board presentations and relationships with CISOs is an important yet early-stage topic. One colleague stated, we are "10 years from maturity" on metrics. Another stated, we need a "language and framework" for decision-makers in security, much like those for finance, legal, marketing, and sales.

At the Wing summit, one board member argued that CISOs in board presentations should "figure out how you want board members to feel" about the security position and plans. Board members are generally not comfortable with security and often walk away from security presentations unsure of "how to feel."

2) Point Solutions. Numerous CISOs discussed the fragmented vendor ecosystem in security. One joked, "there are six products this year for every problem you do not have, up from four products last year for every problem you did not have." Another commented, "no one is solving the overall problem of how to stitch security together."

3) Data. As stated by a CISO, “security is now at the data plane.” Executives discussed a significant effort around who has what data and what they are doing with it, on a continual basis.

4) Asset Management. Several colleagues discussed understanding the assets within their enterprises as a priority, including not only those within IT but also those within other functional organizations and business units. At the Wing summit, one of the board members emphasized the need to “know 100% of your assets”, to which many CISOs expressed uncertainty and frustration.

5) Cloud Security. Cloud migration and security is a clear top priority for the upcoming year. As one colleague said, “everyone wants to figure out network-like security in the new cloud.” Another stated, “cloud is my #1 priority for this year.”

6) Insider Threat. Insider threat was one of the most frequently mentioned priorities in our conversations. Although one colleague mentioned a recent specific incident within his company, most mentioned a general need to monitor and identify potentially suspicious behavior, whether intentional or hacked.

7) Automation. We found divergent perspectives on automation, potentially due to the disparate use cases. Overall, one board member at the Wing summit argued that enterprises are under-investing in automation and that CISOs should “get people out of the loop.” Other perspectives included:

- One CISO discussed making automation “an engineering problem, not a SOC problem.” At his company, automation initiatives had failed under the SOC team, whose positions were conceptually threatened by automation.
- Three CISOs at a private dinner said that they were not convinced of the returns on SOAR. Their deployments had not led to specific metrics, at least yet.
- Another colleague stated, “you can’t automate what you don’t understand.” And, another colleague stated, “be careful about what you automate.”

8) API Security and Security APIs. A major new theme in our meetings was APIs. One colleague discussed the need to discover and monitor all APIs in the enterprise as a new attack surface. Another discussed creating new APIs by the security team for information sharing within the enterprise—organized into three main categories: 1) GRC, 2) SOC, and 3) Engineering.

9) Third-Party. Third-party and supply chain remain a significant topic, as also discussed in last year’s research note. Of the three board members at the Wing summit, two had experienced third-party breaches. In both cases, the third-party was not covered or discussed in the news. One member stated, “it is viewed as your data, whether it is in your systems or someone else’s.”

Other notable comments during our meetings included:

Risk Management. Several colleagues discussed framing security risks in broader context of business risks—with the scenarios and the business cases for investment

decisions such that business owners make “conscious” decisions on security investment trade-offs.

Ransomware. Ransomware was a key theme in several of the keynotes, including the Genomics keynote which we moderated. Healthcare information is more valuable than financial information for hackers, and healthcare is the most breached industry annually—with ransomware as one of the hackers’ exploits.

Employee Training. Several in our meetings emphasized the need to better improve employee education. As one colleague stated, “the endpoint is the user” and “user hardening” is critical to improving security.

Identity. Identity is another major topic in security. One colleague discussed a “world without Active Directory”. Another discussed an interest in rationalizing “from 8 vendors to 1-2”.

Segmentation. Segmentation was discussed by several colleagues in our meetings, as well as by the speakers at the Wing summit.

Privacy. Privacy is a new major trend in tech, and several private companies are taking early leadership positions. SECURITI.ai was named RSA Conference 2020’s “Most Innovative Startup.”

DevSecOps. Several in our meetings discussed DevSecOps, with an emphasis on the “cultural shift” that is required.

Huawei. The Huawei debate was publicly discussed in several sessions at RSA. Katie Arrington at the Department of Defense reiterated the recommendation against Huawei, while Andy Purdy at Huawei argued that 1) security against backdoor risks is possible and 2) rip and replace will be more costly than expected.

Conclusion

Despite the COVID-19 concerns, RSA 2020 was busy and productive. Security is now an imperative at the board level, and the role of the CISO continues to only increase within organizations. Further, there are unsolved problems in many areas, and entrepreneurs and startups continue to play a central part in innovation for the security industry.

Wing Venture Capital is an early stage venture capital firm focused on seed and series A investments in business technology. As disclosure, a list of Wing’s portfolio companies is available on Wing’s website at wing.vc/companies.

We would like to thank Bryce Tolman for his research and contribution to Wing Summit: Security 2020 and this research note on RSA 2020.

Appendix – RSA 2020 Selected Announcements

Application Security

- **42Crunch:** launched its new self-registration feature for API Security Platform, allowing teams to deliver security across the entire API lifecycle.
- **Checkmarx:** announced new enhancements to its Software Security Platform to empower more seamless implementation and automation of application security testing (AST) in modern development and DevOps environments.
- **F5:** introduced its customer-focused approach to Application Protection, bolstered by new offerings and the company's recent acquisition of Shape Security.
- **F5:** highlighted several new solutions in its application security portfolio, including Essential App Protect, Behavioral App Protect, NGINX App Protect, and Aspen Mesh Secure Ingress.
- **Google:** announced the general availability of Web Risk API, which allows web applications to check URLs against Google's constantly growing list of unsafe sites.
- **Imperva:** announced Advanced Bot Protection, a new solution that fully integrates its industry-leading bot management technology into the Imperva Cloud Application Security solution.
- **Intel:** announced that Intel Software Guard Extensions (Intel SGX) will expand to a broader range of mainstream data-centric platforms, providing larger protected enclaves and extending protections to offload accelerators and improved performance.
- **Intertrust:** launched whiteCryption Secure Key Box (SKB) for Web, an enterprise-ready white-box cryptography solution for web applications, which ensures that web apps can be used without fear of exposing the underlying keys and credentials to cyberattack.
- **Proofpoint:** announced innovations on Proofpoint Cloud App Security Broker (CASB) to help secure applications such as Microsoft Office 365, Google's G Suite, Box, Slack, and Amazon Web Services.
- **Spirion:** announced the release of its new SaaS platform, Data Privacy Manager.
- **Unisys:** announced the immediate availability of the new Unisys TrustCheck SaaS Platform to quickly and easily assess the potential financial impact of cyber risks.
- **VMware:** announced enhancements to VMware Carbon Black Cloud, including automated correlation with MITRE ATT&CK framework Technique IDs (TIDs), integration with the Microsoft Windows Anti-Malware Scanning Interface (AMSI), and addition of malware prevention capabilities for Linux machines.
- **WhiteOps:** announced the release of Application Integrity, a new offering designed to protect enterprises from sophisticated bot-based threats including account takeover, automated account creation, and web scraping.

Cloud Security

- **Cisco:** unveiled SecureX, a new cloud-native security platform designed to provide greater visibility across the entire security portfolio.
- **DivvyCloud:** released its 2020 Cloud Misconfigurations Report, which found that nearly 33.4 billion records were exposed in breaches due to cloud misconfigurations in 2018 and 2019, amounting to nearly $5 trillion in costs to enterprises globally.
- **Exabeam:** unveiled the Exabeam Cloud Platform to help security leaders mature their security posture, aid architects to secure new use cases by expediting the provisioning and consumption of new applications, tools and content, and make security engineers and analysts more efficient with simplicity of use and deployment.

- **FireEye:** announced new cloud security innovations, including expanded capabilities within the FireEye Helix platform, as well as FireEye Messaging Security, a new offering that protects collaboration tools such as Microsoft Teams and Slack.
- **FireMon:** released its 2020 State of Hybrid Cloud Security Report, which finds that while enterprises rapidly transition to the public cloud and complexity is increasing, visibility and team sizes are decreasing while security budgets remain flat.
- **Humio:** launched Humio Bucket Storage, making cloud deployments less expensive, faster, and easier to run by using bucket storage for retaining data.
- **McAfee:** announced new innovations to MVISION with the availability of Unified Cloud Edge, which protects enterprise data across devices, web and the Cloud; Cloud Native Infrastructure Security, which helps organizations protect the entire infrastructure and application stack of cloud-native applications; and global Managed Detection and Response (MDR) offering.
- **McAfee:** announced eight new partnerships and seven new certified integrations to McAfee Security Innovation Alliance (SIA) and McAfee CASB Connect Program, giving organizations a competitive advantage to secure people, devices and data in the cloud.
- **McAfee:** announced new innovations to its cloud-native MVISION platform with the availability of Unified Cloud Edge (UCE), which provides unified data and threat protection from device level to the cloud.
- **Menlo Security:** launched its 100% malware protection warranty, offering a warranty of up to $1 million to cover its customers' expenses if a malware attack is able to pass through the company's Isolation Core and cause an infection.
- **MITRE Engenuity:** announced it will assess commercial cybersecurity products against the threat posed by the groups commonly known as Carbanak and FIN7.
- **Protegrity:** announced a new Data Protection Jumpstart Subscription program, which streamlines time-to-live for enterprises adopting the Protegrity Data Security Platform, by condensing the project scope, training, discovery, design, and delivery phases into a 16-week timeframe.
- **RSA Security:** announced availability of RSA Archer SaaS for customers seeking to implement the RSA Archer Suite in the cloud.
- **Secureworks:** launched its new cloud configuration assessment based on VMware Secure State.
- **SentinelOne:** announced the general availability of its next generation container and cloud-native workload protection (CWPP) offering.
- **Tufin:** launched SecureCloud, a security policy automation service that unifies cloud security policy management for container, microservices, and hybrid cloud environments in a single solution, giving organizations greater visibility and control of cloud security.

Endpoint Security

- **Adaptiva:** announced Endpoint Health, its automated endpoint health and remediation solution for clients and servers.
- **Blackberry:** announced new product enhancements to the endpoint protection platform (EPP) and endpoint detection and response (EDR) pillars of its BlackBerry Spark platform.
- **CrowdStrike:** announced CrowdStrike Endpoint Recovery Services, which combines the power of the CrowdStrike Falcon platform, threat intelligence, and real-time response to accelerate business recovery from cyber intrusions.
- **Cyware Labs:** announced version 2.0 enhancements across the matrix of Cyware's solutions, including end-to-end threat intelligence automation, threat response and management capabilities, as well as an improved user interface (UI).

- **VMware:** unveiled that VMware Advanced Security for Cloud Foundation will inject Carbon Black's workload protection Real-time Workload Audit/Remediation technology as well as its Next-Generation Antivirus (NGAV) and Endpoint Detection & Response (EDR) solutions.

Identity and Access Management

- **BrandShield:** launched ElectionShield, which was developed to protect political campaigns around the World from threats including fraudulent fundraising sites, phishing, social phishing, and impersonation.
- **Entrust Datacard:** announced two new high-assurance offerings for the company's unified authentication management platform: Passwordless Single Sign On (SSO) Authentication to improve workforce security and productivity, and Identity Proofing with fully digital identity verification for accelerated customer acquisition and onboarding.
- **Fortanix:** announced that Fortanix Self-Defending Key Management Service (SDKMS) is available on VMware Cloud Marketplace.
- **Google:** announced the general availability of reCAPTCHA Enterprise, the system used to verify login requests that come from legitimate users.
- **GreatHorn:** unveiled a biometric solution that effectively identifies compromised accounts and blocks takeover attempts by validating users with their unique typing patterns.
- **HID Global:** announced a new USB-C option for HID Global's HID Crescendo Key Series family, which features an end-to-end approach to passwordless authentication.
- **Idex Biometrics:** announced it is launching a biometric-system-on-chip (BSoC) to lower the manufacturing cost of biometric smart cards to a point that enables mass market adoption.
- **Kingston Digital:** announced its IronKey D300 Encrypted USB Flash Drive series has achieved NATO Restricted Level Certification.
- **PencilData:** announced the availability of Chainkit for Splunk and Chainkit for Elastic, which applies PencilDATA's distributed ledger-based event log authentication against adversarial anti-forensic techniques used in most successful cyber attacks.
- **Pindrop:** launched Deep Voice 3, which is built on advanced machine learning and deep neural networks and is designed to more accurately recognize the voice of callers at a contact center with less speech.
- **Portnox:** announced that it has partnered with Distology for the sole distribution and resell of its cloud-delivered NAC-as-a-Service solution in the United Kingdom and Ireland.
- **RSA Security:** announced the general availability of RSA Adaptive Authentication for eCommerce version 20.5.

IoT

- **CyberX:** announced a new API-level integration with Microsoft Azure Security Center for IoT, enabling joint clients to gain a unified view of security across all their managed and unmanaged IoT devices.
- **Essence SigmaDots:** announced it has developed a cybersecurity solution that harnesses the power of distributed architecture to completely secure IoT devices, applications, and data.
- **Jitsuin:** announced that it has joined the Ping Identity Technology Alliance Program to extend Identity and Access controls into IoT using the Digital Security Twin.
- **Nozomi Networks:** announced its v20.0 product portfolio release, which includes new groundbreaking anomaly detection technology that delivers unmatched accuracy for enterprise IoT networks.

Messaging Security

- **Microsoft:** announced the availability of campaign views and compromise detection and response.
- **Mimecast:** announced it has added new capabilities to its cloud-based platform comprised of integrated service components that organizations' need to combat the latest cybersecurity challenges.
- **Proofpoint:** announced an integrated, end-to-end solution that addresses BEC and EAC.
- **Trustifi:** incorporated a new AI-enabled feature into its industry-leading email encryption and DLP (data loss prevention) solution that also works via Optical Character Recognition technology (OCR).
- **Valimail:** announced the general availability of Valimail DMARC Monitor a free, cloud-based solution that gives domain owners full visibility into all the services sending email from their domains.

Mobile Security

- **JetPatch:** announced JetPatch version 4.0, allowing IT teams to run a much faster simulation of the patching process before deploying the actual patch cycle.
- **Zimperium:** announced it finished 2019 with triple digit growth in new customer acquisitions, innovative product enhancements, and new strategic partnerships and alliances.

MSSP

- **BishopFox:** launched its Continuous Attack Surface Testing (CAST) managed security service, a subscription service that combines a next-generation attack platform with expert-driven penetration tests to deliver unprecedented visibility into an organization's security posture.
- **DFLabs:** announced the availability of IncMan 5.0, providing clients and partners with an optimized platform with unprecedented speed and flexibility, increasing automation speed well above 70%.
- **esentire:** announced the availability of esCLOUD, a comprehensive portfolio of cybersecurity services which extends their MDR capabilities and elite threat hunting expertise into modern cloud environments.
- **FireEye:** announced the availability of FireEye Mandiant Threat Intelligence Suite.
- **LookingGlass Cyber Solutions:** launched advanced services and features as part of its Cyber Guardian Network.

Network and Infrastructure Security

- **BigID:** introduced new data security capabilities to address critical cybersecurity use cases—empowering customers to protect crown jewel data, discover dark data, automate labelling and policy enforcement, leverage access insight to highlight security vulnerabilities and overexposed data and remediate risk on their most sensitive data.
- **BitSight:** announced BitSight Attack Surface Analytics, a new Security Performance Management solution for security and risk leaders to quickly validate their organizations' digital footprint, assess security posture and cyber risk reputation, and take steps to reduce their cyber risk exposure.
- **CrowdStrike:** announced it is expanding the industry-leading visibility of the CrowdStrike Falcon platform, to protect workloads, across all environments, including workloads and containers running in the cloud and in private, public and hybrid data centers or on-premise.

- **FireMon:** announced expanded capabilities for API integrations with ServiceNow, Cisco ACI and Swimlane to help customers improve network security visibility, control, and efficiency while maximizing the value of their investments in security and IT service management systems.
- **Intel:** announced portfolio for 5G network infrastructure, including the launch of the new Intel Atom P5900, a 10nm system-on-chip (SoC) for wireless base stations.
- **Intel:** launched the new 2nd Gen Intel Xeon Scalable processors to deliver increased value for customers across their cloud, network and edge needs.
- **Juniper Networks:** announced encrypted traffic analysis for Juniper Advanced Threat Prevention (ATP) Cloud and SRX Series firewalls, as well as the integration of SecIntel to the Mist platform for wireless access.
- **Mellanox Technologies:** announced the immediate general availability of ConnectX-6 Dx SmartNICs, in addition to the soon-to-be-released BlueField-2 I/O Processing Units (IPUs).
- **Randori:** introduced Randori Attack Platform, which effectively packages the Red Team concept as a service.
- **RSA Security:** released the latest version of RSA NetWitness Platform, which includes functionality updates for automated network detection and response, user and entity behavior analytics (UEBA) and threat intelligence.
- **Spirent Communications:** announced a new release of CyberFlood Data Breach Assessment, Spirent's solution for evaluating the ability of an organization's security infrastructure to detect active attackers and vulnerabilities.

Recognition

- **Attivo:** named a Grand Trophy Winner in Info Security Products Guide's 16th annual 2020 Global Excellence Awards.
- **Attivo:** received five InfoSec Awards from Cyber Defense Magazine: Best Product in Cloud Security, Cutting Edge Endpoint Security, Most Innovative Deception-Based Security, and Next Gen Insider Threat Detection.
- **Attivo:** named a Hot Company in Critical Infrastructure Protection.
- **Attivo:** received six 2020 Cybersecurity Excellence Awards—Advanced Persistent Threat (APT) Protection, Critical Information Security, Endpoint Detection and Response, Deception Technology, Serverless Security, and Insider Threat Solution.
- **CyberSaint:** announced that it has been named the Gold Winner of five Cybersecurity Excellence Awards for demonstrating extraordinary innovation and leadership in information security.
- **CyberSaint:** announced that it has been named the Silver Winner of the Info Security Product Guide Award for leading IT Governance, Risk and Compliance product.
- **Cymatic:** recognized as the gold award winner for the Cybersecurity Excellence Awards in three top categories: best start-up, most innovative company, and best web application security.
- **CyberArk:** named as the 2020 SC Award winner for Best Enterprise Security Solution, for the second year in a row.
- **Devo Security:** received three awards for Devo Security Operations, the company's new platform that transforms the security operations center (SOC) and scales security analyst effectiveness: the Editor's Choice Award for SIEM from Cyber Defense Magazine, the Info Security Product Guide's Global Excellence Awards Silver Award for SIEM, and recognition as one of CSO's "Hottest new cybersecurity products".
- **FireMon:** named its list of "Ignite Partner of the Year" awards: 2019 Growth Partner of the Year – SHI, 2019 Americas Partner of the Year – Presidio, 2019 EMEA Partner of the Year – IBM

Switzerland, 2019 APAC Partner of the Year – AmonSoft, 2019 Americas Distributor of the Year – SYNNEX, and 2019 International Distributor of the Year – StarLink.

- **Gurucul:** announced that its Gurucul Unified Security & Risk Analytics platform was named Best Product for Insider Threat Prevention in the Cyber Defense InfoSec Awards for 2020.
- **LinkShadow:** won the InfoSec 2020 award by Cyber Defense Magazine.
- **LogMeIn:** awarded Best Product in Identity and Access Management for its LastPass Identity platform from Cyber Defense Magazine.
- **Lucy Security:** announced it has been named a Gold Winner for three 2020 Cybersecurity Excellence Awards, including Best Anti-Phishing, Best Security Education, and Best Security Education Platform.
- **Medigate:** announced that it has received two 2020 InfoSec Awards from Cyber Defense Magazine— “Hot Company for Cybersecurity IoT” and “Best Product for Healthcare IoT Security."
- **Menlo Security:** announced it has won the Cutting-Edge Anti-Malware award and was named Editor’s Choice for SaaS/Cloud Security from Cyber Defense Magazine.
- **Nuance Communications:** announced it has been recognized for Most Innovative Biometrics by Cyber Defense Magazine.
- **Onfido:** announced it has won Best Product for Next Gen Fraud Prevention from Cyber Defense Magazine.
- **RSA Conference:** announced that two world-renowned cryptographers, Professor Joan Daemen and Professor Vincent Rijmen, are the recipients of its annual award for Excellence in the Field of Mathematics.
- **SCADAfence:** awarded for Cutting Edge ICS/SCADA Security, Next Gen Critical Infrastructure Protection, and Cutting Edge Compliance by Cyber Defense Magazine.
- **SECURITI.ai:** won the title of Most Innovative Startup at the RSA Conference 2020 Innovation Sandbox contest.
- **Signal Sciences:** named a January 2020 Gartner Peer Insights Customers’ Choice for Web Application Firewalls (WAF).
- **Silverfort:** announced that it has won the Most Promising Cybersecurity Startup of the Year and the Most Innovative Identity and Access Management award from Cyber Defense Magazine.
- **SparkCognition:** announced today that CRN, a brand of The Channel Company, has named SparkCognition to its annual Security 100 list.
- **STEALTHbits:** awarded multiple Cybersecurity Excellence Gold Awards, including the coveted Best Cybersecurity Company and Best Privileged Access Management Product Award.
- **Stellar Cyber**: announced that it has won the Editor’s Choice – Cybersecurity Artificial Intelligence award from Cyber Defense Magazine.
- **The Cybersecurity Go To Market Dojo:** awarded the Cybersecurity marketing community, including Best Marketing Campaign of the Year, Thought Leadership or Demand Generation to Attivo Networks, Digital Shadows, SentinelOne, Kenna Security, and Pulse Secure
- **Threat Stack:** announced it has won the Cutting Edge Cloud Security Award from Cyber Defense Magazine.
- **Waratek:** announced it has received a 2020 InfoSec Award in the Cutting-Edge Web Application Security category.
- **White Ops:** announce it was awarded two awards from Cyber Defense Magazine.

Risk & Compliance

- **Anitian:** announced Documentation Automation, an enhancement to its Cloud Security Platform that automates documentation for the most stringent compliance standards.

- **AV-Comparatives:** introduced a methodology for testing enterprise-class EDR systems to evaluate the effectiveness systems in detecting and monitoring attacks and providing reporting and remediation functions.
- **Axonius:** launched Cloud Asset Compliance, leveraging data aggregated from public cloud providers to automatically determine how cloud workloads, configuration details, and accounts comply with industry security benchmarks.
- **Beyond Security:** announced that beSECURE will provide the ability to continuously check and report on the vulnerability, topology and configuration of OT networks such as DCS and SCADA.
- **CybelAngel:** announced it has significantly strengthened its digital risk management SaaS platform to detect data leaks and respond to digital threats by expanding its coverage of internet perimeters.
- **Gurucul:** announced Gurucul Unified Security and Risk Analytics, a cloud-native data science driven platform that unifies key Cyber Defense Center functions to enable contextual, risk-prioritized decisions for automating security controls.
- **LogicGate:** announced the LogicGate Integration suite, a collection of integrations with tools that feed valuable risk data into LogicGate applications or bolster workflow by improving efficiency.
- **Microsoft:** announced availability of Insider Risk Management, which leverages AI and machine learning to identify anomalies in user behavior and flag high-risk activities.
- **NSS Labs:** launched a new product ratings system to inform consumers about a product's capacity to meet its obligations, enhancing transparency and enabling consumers to focus on considerations that are most critical to their organizations.
- **Panaseer:** launched availability of continuous Business Risk Perspectives.
- **ReliaQuest:** announced Verify, a new core capability of the GreyMatter platform that offers enterprises a turnkey approach to cyber assurance through continuous attack simulations across on premise and multi-cloud environments.
- **Riskonnect:** announced that it has formed a new, strategic partnership with Compliance.ai, a regulatory change management company, to enable organizations to simplify and streamline their end-to-end compliance processes.

Security Operations

- **Arctic Wolf:** announced the addition of Dan Larson as Senior Vice President of Marketing.
- **Devo Technology:** announced Devo Security Operations, a security operations solution to combine critical security capabilities together with auto enrichment, threat intelligence community collaboration, a central evidence locker, and a streamlined analyst workflow.
- **Guardicore:** announced several new capabilities in its Guardicore Centra Security Platform designed to help security architects visualize, segment, and protect cloud-native applications.
- **Intel:** announced four new security capabilities and provided further information on its Compute Lifecycle Assurance supply chain transparency initiative.
- **Keysight Technologies:** announced Breach Defense, which enables network and security operations teams to measure the effectiveness of operational security by safely simulating the latest attacks and exploits on live networks.
- **Microsoft:** announced availability of new security-awareness training in partnership with Terranova to include Terranova's phishing-related training set in Office 365 Advanced Threat Protection Plan 2.
- **Microsoft:** announced new enhancements for Microsoft Azure Sentinel, designed to deliver instant value and increased efficiency for security operations teams.
- **PreEmptive Solutions:** announced the release of JSDefender, a tool used by software developers to protect JavaScript code from hacking, reverse engineering, and IP and data theft.
- **QuoLab Technologies:** launched a collaborative, data-centric security operations platform.

- **ReversingLabs:** announced new and enhanced capabilities for its Titanium Platform, including new machine learning algorithm models, explainable classification and out-of-the-box security information and event management (SIEM) plug-ins, security, orchestration, automation and response (SOAR) playbooks, and MITRE ATT&CKTM Framework support.
- **SafeBreach:** announced the release of two powerful new capabilities, Risk-Based Vulnerability Management integration and Cloud Native Container Security, to address the problems that face SecOps and DevOps teams.
- **SaltStack:** announced several new features and capabilities introduced in version 6.2 of SaltStack Enterprise, SaltStack Protect, and SaltStack Comply.
- **Scythe:** introduced the SCYTHE Marketplace, which opens SCYTHE's synthetic malware creation platform to trusted third party developers so that they can turn their experience and expertise into new capabilities for a vibrant security ecosystem.
- **Securonix:** launched the Securonix Analytics Sandbox capability, providing an isolated test or QA environment within the production setup for security operations teams to test, tune, and validate new use cases prior to pushing them to live production.
- **SIRP Security Score:** launched a new security scoring module, S3, which calculates an organization's security score based on a number of internal and external factors.
- **Sumo Logic:** announced the availability of its new Cloud SIEM Enterprise offering, which includes a rich set of capabilities to ease the burden on security operations center (SOC) personnel.
- **Synopsys:** introduced the Polaris Software Integrity Platform, which brings the power of Synopsys Software Integrity products and services together into an integrated solution that enables security and development teams to build secure, high-quality software faster.
- **Veracode:** launched the next-generation of Veracode Static Analysis, which features comprehensive analysis across the development lifecycle, including a new Pipeline Scan that is optimized for use when code is submitted to the build process.
- **Veracode:** announced Veracode Security Labs, which teaches secure coding practices through interactive web apps based on modern threats that developers exploit and patch.

Threat Detection and Response

- **Code42:** announced enhancements to its cloud data security solution to equip security teams to closely monitor, detect, and investigate data threats caused by high-risk employees.
- **CounterCraft:** unveiled version 2.6 of its Cyber Deception Platform to help threat hunters and engage with threat actors using controlled synthetic environments.
- **CyberArk:** released privilege-based deception capabilities designed to defend against credential theft on workstations and servers.
- **Elastic:** showcased its integrated threat prevention, collection, detection, and response solution.
- **ExtraHop:** announced new capabilities that provide 360-degree threat visibility, detection, and response across multi-cloud, datacenter, and IoT deployments in a single hosted solution.
- **FireMon:** announced new integrations with Microsoft Azure and AWS to help improve cloud visibility, reduce complexity and match the pace needed to protect systems from ongoing cyber threats and data breaches.
- **Fortinet:** announced FortiAI, an on-premises appliance that leverages self-learning Deep Neural Networks to speed threat remediation and handle time consuming, manual security analyst tasks.
- **Google:** announced two additions to Chronicle—threat detection using the new YARA-L rules language and enhanced data modeling.
- **Gurucul:** introduced automated intelligent threat hunting that uses AI and ML to detect behaviors associated with cyber attacks and data breaches.

- **McAfee:** announced that it is launching a global Managed Detection and Response (MDR) platform, with DXC Technology as McAfee's first strategic MDR partner.
- **Microsoft:** announced availability of Microsoft Threat Protection, enabling security operations teams to get a correlated, incident-level view of threats, instead of managing individual alerts.
- **Palo Alto Networks:** introduced Cortex XSOAR, an extended security orchestration, automation and response platform that empowers security leaders with instant capabilities against threats across their entire enterprise.
- **Trustwave:** announced continued growth and leadership driving cybersecurity threat detection and response initiatives across enterprises and government agencies worldwide.
- **Virsec:** announced it has extended its Verse Security Platform with integrated attack simulation, automated vulnerability detection, and continuous security monitoring during application runtime.
- **VMWare:** adding a new, flexible remediation framework to VMware Secure State to help customers automate actions across multiload environments.

Threat Intelligence

- **Code42:** released its 2020 Data Exposure Report on insider threat, finding that cloud-based collaboration technologies and workforce turnover have become major drivers of data exfiltration.
- **Farsight Security:** announced enhancements to its flagship Security Information Exchange (SIE) data-sharing platform to help security professionals measurably improve the prevention, detection and response to the latest cyberattacks.
- **Fidelis:** announced the latest release of the Fidelis Elevate platform.
- **FireEye:** released the FireEye Mandiant M-Trends 2020 report, which shares statistics and insights gleaned from FireEye Mandiant investigations around the globe in 2019.
- **Imperva:** launched the Cyber Threat Index, a monthly report and measurement of the global threat landscape based on data from Imperva sensors across the globe.
- **Verodin:** operationalized its Threat Intelligence with Threat Actor Assurance Module (TAAM), where organizations can definitively determine their ability to detect, block and alert based on the latest threat actors and their attack behaviors.
- **White Ops:** announced the formation of the Satori Threat Intelligence and Research Team, a specialized team dedicated to researching the threats and trends that organizations are facing from sophisticated bot attacks.

Venture Capital

- **BluBracket:** raised a $6.5 million seed round lead by Unusual Ventures, with participation by Point72 Ventures, Signal Fire and Firebolt Ventures, and introduced its product suite of security code in the enterprise.
- **Netskope:** announced that the company has closed a new $340 million investment led by new investor Sequoia Capital Global Equities at a valuation of nearly $3 billion.
- **Trebel:** announced the formation of a cybersecurity practice group to promote mission-driven, innovative companies in the cybersecurity industry.
- **Zero Networks:** announced it has raised $4.65 million in seed funding, led by F2 Capital and Pico Venture Partners, and unveiled the Zero Networks Access Orchestrator, a network security platform that automatically defines, enforces and adapts user- and machine-level network access policies to create a continuous airtight zero trust network model, at scale.